



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/040,087	04/15/2002	Darrel J. Van Buer	1044-404-01	8837
20583	7590	12/13/2005	EXAMINER	
JONES DAY 222 EAST 41ST ST NEW YORK, NY 10017			SMITHERS, MATTHEW	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 12/13/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/040,087	VAN BUER, DARREL J.	
	Examiner	Art Unit	
	Matthew B. Smithers	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 15 April 2002.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-110 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-110 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| Paper No(s)/Mail Date <u>01/04/2002</u> . | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

The information disclosure statement filed January 4, 2002 has been placed in the application file and the information referred to therein has been considered as to the merits.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-110 are rejected under 35 U.S.C. 102(e) as being anticipated by U.S. patent application 2003/0108195 granted to Okada et al.

Regarding claim 75, Okada meets the claimed limitations as follows:

“An encryption/decryption method comprising:

performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the series of stages;

holding the stage input data block for input into a stage of the series of stages, the input data block having the first selected width;” see page 2, paragraphs [0028] to page 3, paragraph [0039] and page 3, paragraphs [0056] and [0058].

“encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width;” see page 4, paragraph [0060] to paragraph [0069].

“decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption step;” see page 5, paragraph [0070] to paragraph [0080].

and performing a substitution operation on either the encrypted stage input data block or the decrypted stage input data block.” see page 13, paragraph [0163] to paragraph [0165]; Figures 1 and 9 (SubByte –substitution step).

Regarding claim 76, Okada meets the claimed limitations as follows:

“The method of claim 75, further comprising: selecting as a subsequent stage input data block for the subsequent stage of the series of stages the output of the substitution step or the stage input data block.” see page 4, paragraph [0062].

Regarding claim 77, Okada meets the claimed limitations as follows:

“The method of claim 76 further comprising: performing in series the stages of the encryption/decryption operations in a first plurality of stages of the series of stages, each of the stages of the first plurality of stages comprising a round, and repeating this operation for a selected number of times and for a selected number of rounds each of

the selected number of times, to thereby effect a total number of rounds." see page 4, paragraph [0064] to paragraph [0069].

Regarding claim 78, Okada meets the claimed limitations as follows:

"The method of claim 76 further comprising: performing in series the stages of the encryption/decryption operations in a first plurality of stages of the series of stages, each of the stages of the first plurality of stages comprising a round, and repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds." see page 4, paragraph [0064] to paragraph [0069].

Regarding claim 79, Okada meets the claimed limitations as follows:

"The method of claim 77 further comprising: performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary." see page 4, paragraph [0064] to paragraph [0069] and page 6, paragraph [0089] to page 7, paragraph [0093].

Regarding claim 80, Okada meets the claimed limitations as follows:

"The method of claim 78 further comprising: performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary." see page 4, paragraph [0064] to paragraph [0069] and page 6, paragraph [0089] to page 7, paragraph [0093].

Regarding claim 81, Okada meets the claimed limitations as follows:

"The apparatus of claim 75 further comprising: providing a round encryption or decryption key of the first selected width for combination with the block data of the first

selected width, based upon an initial encryption or decryption key of a second selected width." see page 4, paragraphs [0064], [0065] (Next, in rounds 2 through (Nr-1) . . . the number of rounds will differ according to key length) and page 10, paragraphs [0138] to page 11, paragraph [0139].

Regarding claim 82, Okada meets the claimed limitations as follows:

"The method of claim 76 further comprising: providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width." see page 4, paragraphs [0064], [0065] (Next, in rounds 2 through (Nr-1) . . . the number of rounds will differ according to key length) and page 10, paragraphs [0138] to page 11, paragraph [0139].

Regarding claim 83, Okada meets the claimed limitations as follows:

"The method of claim 77 further comprising: providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width." see page 4, paragraphs [0064], [0065] (Next, in rounds 2 through (Nr-1) . . . the number of rounds will differ according to key length) and page 10, paragraphs [0138] to page 11, paragraph [0139].

Regarding claim 84, Okada meets the claimed limitations as follows:

"The method of claim 78 further comprising: providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width."

see page 4, paragraphs [0064], [0065] (Next, in rounds 2 through (Nr-1) . . . the number of rounds will differ according to key length) and page 10, paragraphs [0138] to page 11, paragraph [0139].

Regarding claim 85, Okada meets the claimed limitations as follows:

"The method of claim 79 further comprising: providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width."

see page 4, paragraphs [0064], [0065] (Next, in rounds 2 through (Nr-1) . . . the number of rounds will differ according to key length) and page 10, paragraphs [0138] to page 11, paragraph [0139].

Regarding claim 86, Okada meets the claimed limitations as follows:

"The method of claim 80 further comprising: providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width."

see page 4, paragraphs [0064], [0065] (Next, in rounds 2 through (Nr-1) . . . the number of rounds will differ according to key length) and page 10, paragraphs [0138] to page 11, paragraph [0139].

Regarding claim 87, Okada meets the claimed limitations as follows:

"The method of claim 81, further comprising: generating each round key by the expansion of a starting key of a second selected width." see page 9, paragraphs [0127] to page 12, paragraph [0156].

Regarding claim 88, Okada meets the claimed limitations as follows:

"The method of claim 82, further comprising: generating each round key by the expansion of a starting key of a second selected width." see page 9, paragraphs [0127] to page 12, paragraph [0156].

Regarding claim 89, Okada meets the claimed limitations as follows:

"The method of claim 83, further comprising: generating each round key by the expansion of a starting key of a second selected width." see page 9, paragraphs [0127] to page 12, paragraph [0156].

Regarding claim 90, Okada meets the claimed limitations as follows:

"The method of claim 84, further comprising: generating each round key by the expansion of a starting key of a second selected width." see page 9, paragraphs [0127] to page 12, paragraph [0156].

Regarding claim 91, Okada meets the claimed limitations as follows:

"The method of claim 85, further comprising: generating each round key by the expansion of a starting key of a second selected width." see page 9, paragraphs [0127] to page 12, paragraph [0156].

Regarding claim 92, Okada meets the claimed limitations as follows:

"The method of claim 86, further comprising: generating each round key by the expansion of a starting key of a second selected width." see page 9, paragraphs [0127] to page 12, paragraph [0156].

Regarding claim 93, Okada meets the claimed limitations as follows:

"The method of claim 87, further comprising: the second selected width equals the first selected width." see page 9, paragraphs [0127] to page 12, paragraph [0156].

Regarding claim 94, Okada meets the claimed limitations as follows:

"The method of claim 88, further comprising: the second selected width equals the first selected width." see page 9, paragraphs [0127] to page 12, paragraph [0156].

Regarding claim 95, Okada meets the claimed limitations as follows:

"The method of claim 89, further comprising: the second selected width equals the first selected width." see page 9, paragraphs [0127] to page 12, paragraph [0156].

Regarding claim 96, Okada meets the claimed limitations as follows:

"The method of claim 90, further comprising: the second selected width equals the first selected width." see page 9, paragraphs [0127] to page 12, paragraph [0156].

Regarding claim 97, Okada meets the claimed limitations as follows:

"The method of claim 91, further comprising: the second selected width equals the first selected width." see page 9, paragraphs [0127] to page 12, paragraph [0156].

Regarding claim 98, Okada meets the claimed limitations as follows:

"The method of claim 92, further comprising: the second selected width equals the first selected width." see page 9, paragraphs [0127] to page 12, paragraph [0156].

Regarding claim 99, Okada meets the claimed limitations as follows:

"The method of claim 93 further comprising: the encryption step further includes performing an affine transformation and the decryption step further includes performing an inverse of the affine transformation." see page 13, paragraphs [0168] to [0170]

(Expression 1 is an affine transformation and Expression 3 is an inverse affine transformation).

Regarding claim 100, Okada meets the claimed limitations as follows:

"The method of claim 94 further comprising: the encryption step further includes performing an affine transformation and the decryption step further includes performing an inverse of the affine transformation." see page 13, paragraphs [0168] to [0170]
(Expression 1 is an affine transformation and Expression 3 is an inverse affine transformation).

Regarding claim 101, Okada meets the claimed limitations as follows:

"The method of claim 95 further comprising: the encryption step further includes performing an affine transformation and the decryption step further includes performing an inverse of the affine transformation." see page 13, paragraphs [0168] to [0170]
(Expression 1 is an affine transformation and Expression 3 is an inverse affine transformation).

Regarding claim 102, Okada meets the claimed limitations as follows:

"The method of claim 96 further comprising: the encryption step further includes performing an affine transformation and the decryption step further includes performing an inverse of the affine transformation." see page 13, paragraphs [0168] to [0170]
(Expression 1 is an affine transformation and Expression 3 is an inverse affine transformation).

Regarding claim 103, Okada meets the claimed limitations as follows:

"The method of claim 97 further comprising: the encryption step further includes

Art Unit: 2137

performing an affine transformation and the decryption step further includes performing an inverse of the affine transformation.” see page 13, paragraphs [0168] to [0170] (Expression 1 is an affine transformation and Expression 3 is an inverse affine transformation).

Regarding claim 104, Okada meets the claimed limitations as follows:

”The method of claim 98 further comprising: the encryption step further includes performing an affine transformation and the decryption step further includes performing an inverse of the affine transformation.” see page 13, paragraphs [0168] to [0170] (Expression 1 is an affine transformation and Expression 3 is an inverse affine transformation).

Regarding claim 105, Okada meets the claimed limitations as follows:

”An encryption/decryption method comprising:

performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the series of stages;

holding the stage input data block for input into a stage of the series of stages, the input data block having the first selected width;” see page 2, paragraphs [0028] to page 3, paragraph [0039] and page 3, paragraphs [0056] and [0058].

”encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique

combination of data bits for each unique combination of data bits in the stage input data block of the first selected width;" see page 4, paragraph [0060] to paragraph [0069].

"decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption step;" see page 5, paragraph [0070] to paragraph [0080].

"performing a substitution operation on either the encrypted stage input data block or the decrypted stage input data block." see page 13, paragraph [0163] to paragraph [0165]; Figures 1 and 9 (SubByte –substitution step).

"and selecting as a subsequent stage input data block for the subsequent stage of the series of stages the output of the substitution step or the stage input data block." see page 4, paragraph [0062].

Regarding claim 106, Okada meets the claimed limitations as follows:

"An encryption/decryption method comprising:

performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the series of stages;

holding the stage input data block for input into a stage of the series of stages, the input data block having the first selected width;" see page 2, paragraphs [0028] to page 3, paragraph [0039] and page 3, paragraphs [0056] and [0058].

“encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width;” see page 4, paragraph [0060] to paragraph [0069].

“decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption step;” see page 5, paragraph [0070] to paragraph [0080].

“performing a substitution operation on either the encrypted stage input data block or the decrypted stage input data block.” see page 13, paragraph [0163] to paragraph [0165]; Figures 1 and 9 (SubByte –substitution step).

“selecting as a subsequent stage input data block for the subsequent stage of the series of stages the output of the substitution step or the stage input data block.” see page 4, paragraph [0062].

and, performing in series the stages of the encryption/decryption operations in a first plurality of stages of the series of stages, each of the stages of the first plurality of stages comprising a round, and repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds.” see page 4, paragraph [0064] to paragraph [0069].

Regarding claim 107, Okada meets the claimed limitations as follows:

“An encryption/decryption method comprising:

performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the series of stages;

holding the stage input data block for input into a stage of the series of stages, the input data block having the first selected width;" see page 2, paragraphs [0028] to page 3, paragraph [0039] and page 3, paragraphs [0056] and [0058].

"encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width;" see page 4, paragraph [0060] to paragraph [0069].

"decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption step;" see page 5, paragraph [0070] to paragraph [0080].

"performing a substitution operation on either the encrypted stage input data block or the decrypted stage input data block." see page 13, paragraph [0163] to paragraph [0165]; Figures 1 and 9 (SubByte –substitution step).

"selecting as a subsequent stage input data block for the subsequent stage of the series of stages the output of the substitution step or the stage input data block." see page 4, paragraph [0062].

“performing in series the stages of the encryption/decryption operations in a first plurality of stages of the series of stages, each of the stages of the first plurality of stages comprising a round, and repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds.” see page 4, paragraph [0064] to paragraph [0069].

and performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary.” see page 4, paragraph [0064] to paragraph [0069] and page 6, paragraph [0089] to page 7, paragraph [0093].

Regarding claim 108, Okada meets the claimed limitations as follows:

“An encryption/decryption method comprising:

performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the series of stages;

holding the stage input data block for input into a stage of the series of stages, the input data block having the first selected width;” see page 2, paragraphs [0028] to page 3, paragraph [0039] and page 3, paragraphs [0056] and [0058].

“encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width;” see page 4, paragraph [0060] to paragraph [0069].

“decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption step;” see page 5, paragraph [0070] to paragraph [0080].

“performing a substitution operation on either the encrypted stage input data block or the decrypted stage input data block.” see page 13, paragraph [0163] to paragraph [0165]; Figures 1 and 9 (SubByte –substitution step).

“selecting as a subsequent stage input data block for the subsequent stage of the series of stages the output of the substitution step or the stage input data block.” see page 4, paragraph [0062].

“performing in series the stages of the encryption/decryption operations in a first plurality of stages of the series of stages, each of the stages of the first plurality of stages comprising a round, and repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds.” see page 4, paragraph [0064] to paragraph [0069].

“performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary.” see page 4, paragraph [0064] to paragraph [0069] and page 6, paragraph [0089] to page 7, paragraph [0093].

”and, generating each round key by the expansion of a starting key of a second selected width.” see page 4, paragraphs [0064], [0065] (Next, in rounds 2 through (Nr-1)

... the number of rounds will differ according to key length) and paragraph [0139] and page 9, paragraphs [0127] to page 12, paragraph [0156].

Regarding claim 109, Okada meets the claimed limitations as follows:

"An encryption/decryption method comprising:

performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the series of stages;

holding the stage input data block for input into a stage of the series of stages, the input data block having the first selected width;" see page 2, paragraphs [0028] to page 3, paragraph [0039] and page 3, paragraphs [0056] and [0058].

"encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width;" see page 4, paragraph [0060] to paragraph [0069].

"decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption step;" see page 5, paragraph [0070] to paragraph [0080].

“performing a substitution operation on either the encrypted stage input data block or the decrypted stage input data block.” see page 13, paragraph [0163] to paragraph [0165]; Figures 1 and 9 (SubByte –substitution step).

“selecting as a subsequent stage input data block for the subsequent stage of the series of stages the output of the substitution step or the stage input data block.” see page 4, paragraph [0062].

“performing in series the stages of the encryption/decryption operations in a first plurality of stages of the series of stages, each of the stages of the first plurality of stages comprising a round, and repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds.” see page 4, paragraph [0064] to paragraph [0069].

“performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary.” see page 4, paragraph [0064] to paragraph [0069] and page 6, paragraph [0089] to page 7, paragraph [0093].

“generating each round key by the expansion of a starting key of a second selected width and the selected width equals the first selected width.” see page 4, paragraphs [0064], [0065] (Next, in rounds 2 through (Nr-1) . . . the number of rounds will differ according to key length) and paragraph [0139] and page 9, paragraphs [0127] to page 12, paragraph [0156].

Regarding claim 110, Okada meets the claimed limitations as follows:

“An encryption/decryption method comprising:

performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and providing an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the series of stages;

holding the stage input data block for input into a stage of the series of stages, the input data block having the first selected width;" see page 2, paragraphs [0028] to page 3, paragraph [0039] and page 3, paragraphs [0056] and [0058].

"encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width;" see page 4, paragraph [0060] to paragraph [0069].

"decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption step;" see page 5, paragraph [0070] to paragraph [0080].

"performing a substitution operation on either the encrypted stage input data block or the decrypted stage input data block." see page 13, paragraph [0163] to paragraph [0165]; Figures 1 and 9 (SubByte –substitution step).

"selecting as a subsequent stage input data block for the subsequent stage of the series of stages the output of the substitution step or the stage input data block." see page 4, paragraph [0062].

“performing in series the stages of the encryption/decryption operations in a first plurality of stages of the series of stages, each of the stages of the first plurality of stages comprising a round, and repeating this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds.” see page 4, paragraph [0064] to paragraph [0069].

“performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary.” see page 4, paragraph [0064] to paragraph [0069] and page 6, paragraph [0089] to page 7, paragraph [0093].

“generating each round key by the expansion of a starting key of a second selected width.” see page 4, paragraphs [0064], [0065] (Next, in rounds 2 through (Nr-1) . . . the number of rounds will differ according to key length) and paragraph [0139] and page 9, paragraphs [0127] to page 12, paragraph [0156].

“and the encryption step further includes performing an affine transformation and the decryption step further includes performing an inverse of the affine transformation.” see page 13, paragraphs [0168] to [0170] (Expression 1 is an affine transformation and Expression 3 is an inverse affine transformation).

Regarding claim 34, Okada meets the claimed limitations as follows:

” An encryption/decryption circuit comprising:

a staged pipelined logic circuit adapted to perform in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing

an encryption/decryption key of the first selected width and to provide an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit;

a stage input data block buffer adapted to hold the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;" see page 2, paragraphs [0028] to page 3, paragraph [0039] and page 3, paragraphs [0056] and [0058].

"an encryption circuit adapted to encrypt the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit;" see page 4, paragraph [0060] to paragraph [0069] and see page 13, paragraph [0163] to paragraph [0165]; Figures 1 and 9 (SubByte –substitution step).

"a decryption circuit adapted to decrypt the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit;"

see page 5, paragraph [0070] to paragraph [0080] and see page 13, paragraph [0163] to paragraph [0165]; Figures 1 and 9 (SubByte –substitution step).

“a first selector circuit adapted to select as the input to the substitution circuit the first or the second input; a second selector circuit adapted to select as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit the output of the substitution circuit or the stage input data block;” see page 4, paragraph [0062].

“the staged pipelined logic circuit being further adapted to perform in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit, each of the stages of the first plurality of stages comprising a round, and to repeat this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds; the staged pipelined logic circuit being further adapted to perform in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary;” see page 4, paragraph [0064] to paragraph [0069].

“and, a round key generation circuit adapted to provide a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.” see page 4, paragraphs [0064], [0065] (Next, in rounds 2 through (Nr-1) . . . the number of rounds will differ according to key length) and paragraph [0139] and page 9, paragraphs [0127] to page 12, paragraph [0156].

Regarding claim 71, Okada meets the claimed limitations as follows:

" An encryption/decryption circuit comprising:

a staged pipelined logic circuit means for performing in series stages of encryption/decryption operations on a stage data block of a first selected width utilizing an encryption/decryption key of the first selected width and to provide an output data block of the first selected width, comprising a subsequent stage input data block input to a subsequent stage of the staged pipelined logic circuit;

a stage input data block buffer means for holding the stage input data block for input into a stage of the staged pipelined logic circuit, the input data block having the first selected width;" see page 2, paragraphs [0028] to page 3, paragraph [0039] and page 3, paragraphs [0056] and [0058].

"an encryption circuit means for encrypting the stage input data block into a encrypted stage input data block having the first selected width, the encrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width, and the encrypted stage input data block forming an input to a stage substitution circuit, the output of the stage substitution circuit forming a first subsequent stage input data block for a subsequent stage of the staged pipelined logic circuit;" see page 4, paragraph [0060] to paragraph [0069] and see page 13, paragraph [0163] to paragraph [0165]; Figures 1 and 9 (SubByte –substitution step).

"a decryption circuit means for decrypting the stage input data block into a decrypted stage input data block having the first selected width, the decrypted stage input data block comprising a unique combination of data bits for each unique combination of data bits in the stage input data block of the first selected width that is the inverse of the encryption performed by the encryption circuit, the decrypted stage input data block forming a second subsequent stage input to the substitution circuit;" see page 5, paragraph [0070] to paragraph [0080] and see page 13, paragraph [0163] to paragraph [0165]; Figures 1 and 9 (SubByte –substitution step).

"a first selector circuit means for selecting as the input to the substitution circuit the first or the second input; a second selector circuit means for selecting as the subsequent stage input data block for the subsequent stage of the staged pipelined logic circuit the output of the substitution circuit or the stage input data block;" see page 4, paragraph [0062].

"the staged pipelined logic circuit being further means for performing in series the stages of the encryption/decryption operations in a first plurality of stages of the staged pipelined logic circuit, each of the stages of the first plurality of stages comprising a round, and to repeat this operation for a selected number of times and for a selected number of rounds each of the selected number of times, to thereby effect a total number of rounds; the staged pipelined logic circuit being further means for performing in any given one of the first plurality of times less than the first plurality of rounds depending upon the total number of rounds necessary;" see page 4, paragraph [0064] to paragraph [0069].

“and, a round key generation circuit means for providing a round encryption or decryption key of the first selected width for combination with the block data of the first selected width, based upon an initial encryption or decryption key of a second selected width.” see page 4, paragraphs [0064], [0065] (Next, in rounds 2 through (Nr-1) . . . the number of rounds will differ according to key length) and paragraph [0139] and page 9, paragraphs [0127] to page 12, paragraph [0156].

Claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 35, 36 and 37 are apparatus claims adapted to perform the method steps of claims 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, and 110, respectively. Therefore claims 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 35, 36 and 37 are rejected by a similar rationale.

Claims 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 72, 73 and 74 are apparatus claims adapted to perform the method steps of claims 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, and 110, respectively. Therefore claims 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 72, 73 and 74 are rejected by a similar rationale.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

A. Wu et al., “CryptoManiac: A Fast Flexible Architecture for Secure Communication”, discloses a processing techniques for using the Rijndael cipher algorithm.


B. Burke et al., "Architectural Support for Fast Symmetric-Key Cryptography", discloses a method for improving the performance of symmetric key cipher algorithms.

C. Chodowiec et al., "Fast Implementation of Secret-Key Block Ciphers Using Mixed Inner-and Outer-Round Pipelining", discloses a methodology for optimizing the number of pipeline stages in ciphers such as Rijndael.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B. Smithers whose telephone number is (571) 272-3876. The examiner can normally be reached on Monday-Friday (8:00-4:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel L. Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).


Matthew B Smithers
Primary Examiner
Art Unit 2137